PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04M 1/72, G08B 13/14

A1

(11) International Publication Number: WO 97/23986

(43) International Publication Date: 3 July 1997 (03.07.97)

(21) International Application Number: PCT/GB96/03177

(22) International Filing Date: 20 December 1996 (20.12.96)

(30) Priority Data:
9526235.8 21 December 1995 (21.12.95) GB

(71) Applicant *(for all designated States except US)*: BRITISH TECHNOLOGY GROUP LIMITED [GB/GB]; 101 Newington Causeway, London SE1 6BU (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: SANSOME, Andrew, Jonathan, Thomas [GB/GB]; Treetops, Longwood Road, Owslesbury, Winchester SO21 1LL (GB).

(74) Agent: BUTTRICK, Richard; British Technology Group Ltd., Patents Dept., 101 Newington Causeway, London SE1 6BU (GB).

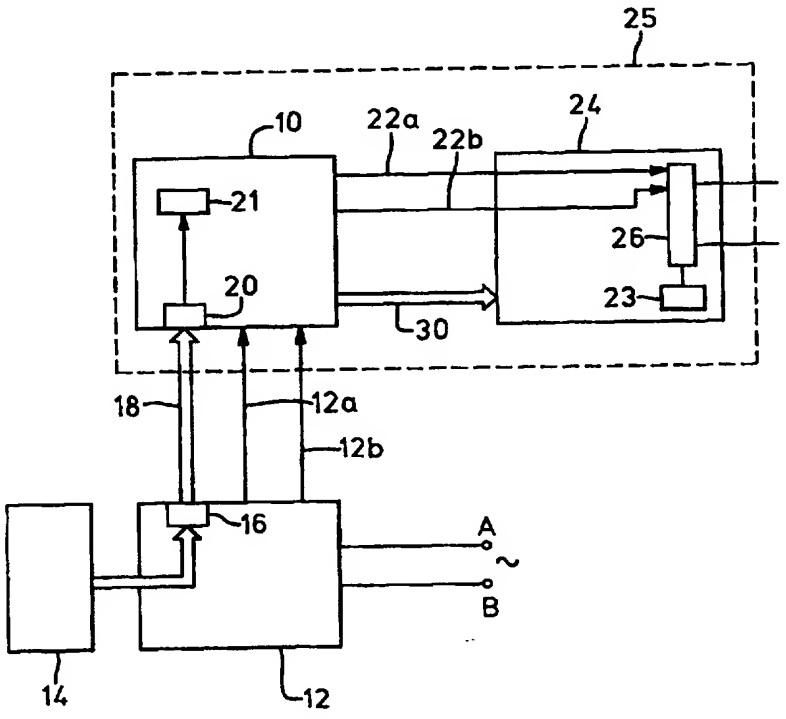
(81) Designated States: CA, JP, KR, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: AN ELECTRONIC ANTI-THEFT APPARATUS AND RELATED METHOD

(57) Abstract

The invention describes an anti-theft apparatus and related method for use with portable electrical or electronic apparatus, particularly with mobile telephones or personal computers. The invention comprises a first data store in which an encrypted code is stored in the electronic apparatus, a comparator and a removable second data store which is within a removable, rechargeable battery unit which unit comprises a battery and a memory store. Upon insertion of the battery unit a security code is transmitted to the first data store. If the code is recognised as a valid authorisation code, the apparatus is enabled and may be operated in the usual way. If it is not recognised the apparatus may be disabled electronically. Once the battery is spent the apparatus is useless, because unless the battery unit receives a refreshed security code upon recharge (from a recharger equipped with a means for re-supplying a suitable code) the electronic apparatus may not be used. Preferably a recharger has been modified such that a valid security code is transmitted to the battery unit at each recharge.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

AN ELECTRONIC ANTI-THEFT APPARATUS AND RELATED METHOD

The present invention relates to an electronic anti-theft apparatus and related method, and in particular, but not exclusively to an anti-theft system for use with portable electronic equipment.

It is unfortunate that in today's society crime appears to be growing. In particular theft is an everyday problem. Often thieves steal high value, portable electronic consumer equipment apparatus, for example portable personal computers, video cameras and mobile telephones. Such apparatus can be expensive to replace and in the case of portable personal computers, the theft of such apparatus can also mean the potential exposure of highly confidential material stored on the computer.

It is an object of the present invention to overcome the above mentioned problem by providing an anti-theft system comprising a method and apparatus, suitable for use with electronic apparatus specifically of the type mentioned above, although it will be understood that the invention can be used with other types of electronic apparatus.

German Offenlegungschrift DE-A1-3803357 (PHILIPS) describes a security system for use with portable electronic equipment. The system consists of a battery charger designated for use with the equipment. The charger has a code transmitter and a code receiver. The code receiver disables the equipment if the code it receives, from the charger, does not match that stored in the code receiver.

The system described is for use with equipment having a built-in, rechargeable battery. A disadvantage of the prior-art system described is that when such an energy source is depleted there may be a considerable time, whilst the battery recharges until the system may be used again. Nowadays, many pieces of mobile electronic equipment are supplied with a second rechargeable battery so that a user may easily swap a charged battery for a depleted one. Such equipment could not be used with the aforementioned recharger because the batteries are not removable.

Another disadvantage with the prior-art system is that it would be possible for an unauthorised person to physically remove (disconnect) a spent battery and replace it with a battery which has been charged using an "unauthorised" charger, as there is no mechanism of verifying the authenticity of a recharged battery.

According to a first aspect of the present invention there is provided apparatus which receives a removable battery unit, the battery unit comprises a rechargeable battery and a memory store, the apparatus having comparison means for comparing a security code stored in the apparatus, with an authorisation code presented by the memory store and means for selectively enabling the apparatus upon receipt of a valid authorisation code or disabling the apparatus upon receipt of an invalid authorisation code.

Once enabled the electronic apparatus will function normally. For example, in the case of a portable telephone, it can be used to make and/or receive calls. However, if the security code is not an authorised code supplied by the battery unit, the electronic apparatus will be disabled. That is to say the apparatus is "jammed" so that it may not be used for its intended purpose. Disabling may be performed electronically.

According to another aspect of the present invention there is provided an electronic electrical or electronic apparatus having a first data store to store a security code (the stored code), means to read an authorisation code; means to compare the authorisation code with the stored code, means to enable operation of the apparatus when the authorisation code is a valid authorisation code, characterised in that the apparatus is adapted to receive a removable, rechargeable battery unit which unit comprises a battery and a memory store.

Conveniently the battery is a rechargeable battery having a volatile memory such as, for example, a Random Access Memory (RAM) or an erasable programmable store, such as, for example, an erasable programmable read only memory (EPROM).

Preferably, the authorisation code originates from a code source which is provided within a battery charger used for recharging the battery and is transmitted to the memory during recharging.

Thus the apparatus is effectively tailored for use with batteries which have been charged with the owner's charger, i.e. an "authorised" charger and as soon as the battery has discharged, unless the correct authorisation code is resupplied, the apparatus may not be used.

Because most portable electrical or electronic apparatus is supplied (in order to reduce weight and size) with one or more removable, rechargeable batteries and a separate battery charger (which is not usually transported or stored with the apparatus), it is apparent

that the present system is more secure and more flexible than the aforementioned system described in DE-A1-3803357.

According to a further aspect of the present invention, there is provided a battery charger for charging a battery, the charger comprising a primary code source, and means responsive to said code source to transmit an authorisation security code to a data store in a battery unit whilst the battery is recharging.

Preferably the battery charger supplies the code during supply of current required to recharge the battery. Alternatively the authorisation security code may be supplied prior to charging or subsequent to charging. The battery unit and battery charger may be configured such that at the commencement of a charging cycle any security code still held in a store within a memory store in the battery unit is first erased and a new security code is written to the store in the battery unit. Such a system has a higher level of security. Similarly the electrical or electronic apparatus may be equipped with a means for automatically erasing the code in the memory store if an attempt is made to gain access to the store in the battery unit. Automatic erasing may be carried out by means in the battery unit or in the apparatus.

According to a further aspect of the invention there is provided a battery unit comprising a rechargeable battery and a data memory store (e.g. an EPROM) within which data memory store an authorisation security code is written.

Preferably the authorisation security code is transmitted to the battery unit when the battery is being recharged.

Preferably, prior to use, the battery unit is required to convey the code more than once having a single cycle and the electronic apparatus is arranged to receive the code more than once.

The security codes may be encrypted in such a way that the possession of both the battery unit (containing the "primary" code and presenting an encrypted form of the authorisation code) and the electronic apparatus containing the security code (to be protected) does not permit identification of any of the codes.

Conveniently, circuitry located in the battery unit is operative to read data, the circuitry comprising: means to identify connection of the battery unit to the charger; means for storing data, which permits erasing of said data when stored; means to decode said data

and means to store serial data after a predetermined period when data is presented by the charger.

Preferably the circuitry provided in the battery unit, includes means to write data to the electrical or electronic apparatus comprising: means to identify connection of an electronic apparatus to the battery unit; means to read stored data; means to encode the data; and means to send the encoded data to the electronic apparatus.

Advantageously said data is used in serial data form. There may also be provided means to read a second piece of data, (second portion of the code), means to encode said data by addition to a subsequent piece of data, generated by a pseudo-random sequence generator, and means to retransmit the subsequently generated authorisation code to the electronic apparatus.

Means may be provided which is adapted to stop transmitting until the battery unit has been removed from the electronic apparatus.

According to a further aspect of the present invention there is provided a method of charging a rechargeable battery unit characterised in that a security code is transmitted to a memory store in the battery unit.

Embodiments of the invention will now be described, by way of example only, and with reference to the Figures in which:

Figure 1 shows an overall block diagram showing the concept of the invention;

Figure 2 is a circuit diagram of a battery charger;

Figure 3 is a circuit diagram of a battery unit; and

Figure 4 is a circuit diagram of an electronic apparatus.

Figure 1 shows diagrammatically a working implementation and is only intended to demonstrate the principles involved. It is not the only way of achieving the broader objective of the invention.

An electronic apparatus 24 comprises a first data store 26 for storing a code; means 23 for comparing a stored code with a security code received from a second data store 21 and means to enable the electronic apparatus 24 when the security code is a valid authorisation code characterised in that the second data store 21 is housed within a detachable rechargeable battery unit 10.

Figure 1 shows a rechargeable battery unit 10, (described below in detail with reference to Figure 3) connected to a battery charger 12 (described below in detail with reference to Figure 2) via power lines 12a and 12b. The battery charger 12 is in turn connected to a mains supply across A, B. A data entry means 14, such as a keypad, is connected, temporarily or permanently, to the battery charger 12. The data entry means 14 passes a coded security signal (the authorisation code) to a memory store 16 housed inside the battery charger 12. The store 16 includes an electronic memory device such as a random access memory (RAM) chip (not shown). The authorisation code (or authorisation code generator) is therefore stored in the battery charger 12. The code is transmitted to a store 21 in the battery unit 10 via a separate data link 18. Alternatively the authorisation code can be transmitted to the battery unit 10 via dedicated connections 12a and 12b.

Figure 4 shows a circuit, which may be a portable personal computer or a telephone.

Electronic apparatus 24 houses the battery unit 10. This is illustrated by the dotted line surrounding a combined portable module 25. Battery unit 10 is detachable and removable from module 25.

The embodiment described in detail below, with reference to Figures 2 to 4, utilises only four bit security with corresponding "random numbers". Therefore it is not as secure as might be desired. As will be appreciated by a skilled person, a commercial implementation may use 8, 12 or even 16 bit random numbers and would therefore be physically only slightly more complex, and otherwise identical. However, it would offer much higher security.

Figure 2 shows how two four bit codes from the battery unit to a mobile electronic apparatus 24 are written to the battery unit 10 by a charger 12 as a single 8 bit word. Charger 12 has an oscillator having resistor 30, capacitor 32, and Schmitt inverter 34 (part of IC1). These produce a clock signal. There is also a counter 40 and a shift register 42 which acts as a parallel to serial converter. Gating means 44 is provided to produce a serial pulse width modulated data stream at output pin 46.

Master clock oscillator 48 (frequency f) runs continually and clocks counter 40. Counter Q1 therefore produces a square wave at f/2. Counter Q5 counts at f/32. (The remaining stages of counter Q5 are not directly relevant to the present invention.)

Counter Q5 is therefore alternately high for a first set of 16 clock pulses and then low for the following set of 16 clock pulses.

Shift register 42 is clocked by counter Q1 (i.e. at f/2 which is half of the master clock rate.). Parallel input lines of shift register 42 are connected either high (to VDD) to represent a ONE or low (to VSS) to represent a ZERO, representing eight bits of data. Thus two four bit code numbers are used by the battery unit 10 and electronic apparatus 24 are programmed by connecting the parallel input lines either high or low. This may be achieved for example with a dip switch (not shown).

Serial / parallel select line, of shift register 42, is connected to Q5 pin of counter 40. When Q5 is high, parallel data on the shift register input lines is jammed in. When Q5 is low the data is shifted out sequentially from QH, at f/2. Thus QH remains at the level of input H for 16 master clock cycles whilst the counter Q5 is high. When Q5 goes low, 8 bits of serial data are presented followed by a low for the next 8 clock cycles. The process is then repeated.

Inverters 50 and 52, "AND" gates 54, 56 and 58 and "OR" gates 60 and 62, combine the master clock with the counter Q1, Q5 and shift register QH so as to produce a pulse width modulated serial data stream at f/2. The pulse length is half of the period of master clock 48, when the data represented is ZERO(0) and 1.5 times the period of master clock 48 when the data represents a ONE (1).

Inverter 64 and "AND" gate 66 block data when the counter Q5 is high, so that the only data to appear at output 46 are the required 8 bits after Q5 goes low. Thus the battery charger 12 produces an 8 bit pulse width modulated data stream representing data programmed onto the input pins of the shift register. This data is repeated every 32 cycles of the master clock 48. It requires 8 clock cycles and is followed by a pause (output data line is low) for 24 clock cycles.

The circuit described above with reference to Figure 2 does not require valid data to be received twice. Such variation to the embodiment is well known to the skilled artisan. The circuit may be readily adapted to perform this function. Namely verification of data upon receipt of two sets of correct data sequences, one after the other, is required in order to enable the apparatus.

Figure 3 shows a circuit diagram of the battery unit. Circuitry which is located in the battery unit 10. It comprises two sections: circuitry to read data from the battery charger 12 and circuitry to write data to the electronic apparatus 24.

Referring to Figure 3 in detail, the battery unit 10 is connected to input line 67 such that the voltage on the input of inverter 70 rises to VDD. Output of inverter 70 goes low producing a positive pulse at the output of inverter 72 which resets counter 74. Q14 of counter 74 is reset low enabling its clock via OR gate 76. Serial pulse width modulated data is presented to monostables 78 and 80 (M/S 78 and M/S 80). In a particularly preferred embodiment the timing can be derived from a master clock (not shown). M/S 78 and M/S 80 are triggered by a positive going edge of an input waveform. M/S 80 is retriggerable and has a period which is slightly greater than that of incoming data. Its "Q" therefore goes high at the start of the eight bits of data and remains high for their duration. M/S 80 Q clocks "D" type latch 82, (D82) transferring the state of its data input (connected to Q5 of counter 74) to its "Q" and thence to "AND" gate 84. Until counter 74 Q5 goes high the data pin of "D" type latch 82 and therefore its Q is low, thereby preventing the transmission of the derived clock via AND 84 to shift registers 86 and 88. Potentially corrupt data is therefore blocked at power on.

At the start of each input data stream (once counter 74 Q5 is high) the NOT Q of D type latch 82 goes low generating a reset pulse to shift registers 86 and 88 via resistor 90, capacitor 92 and inverter 94. This reset can be edge triggered and would not require timing components. Until Q13 of counter 74 goes high, the derived clock is prevented from reaching shift registers 86 and 88 by AND gate 84, preventing new data from being written until charging has continued for a period of 4096 clock cycles. This delay might be set to several minutes to enhance security.

Monostable 78 has a period equal to that of the charger clock. Thus the state of "Data in" line when the NOT Q of monostable 78 goes high, (end of the monostable period) represents data sent from the battery charger 12.

The derived clock via AND gate 84 clocks data from "Data in" into shift registers 86 and 88. Thus during charging, once counter 74 Q13 is high the shift registers are repeatedly reset and loaded with data. When counter 74 Q14 goes high counter 74 clock is inhibited via OR gate 76. At this time the cycle stops, leaving the last set of data

sent in shift registers 86 and 88. The battery unit 10 then remains in this state until either removed from the charger 12 , and reconnected (when the sequence is repeated) or connected to the electronic apparatus 24.

The battery unit has a clock oscillator which comprises invertor 98 capacitor 100 and resistor 102 operates continuously. A pseudo-random sequence generator (P.R.S.) is formed from shift register 104 and exclusive OR gate 106 (XOR 106) . OR gate 108 and NOR gate 110 ensure that the P.R.S. cannot latch in an all LOW state. It produces a sequence of (2^n)-1 numbers of length n bits (where n is the number of stages in the shift register). When the battery unit 10 is disconnected from the electronic apparatus 24 the REQUEST in line remains high via resistor 112, holding reset counter 114 and "D" type latch 116 and enabling the clock to the pseudo-random sequence generator via AND gate 118.

When battery unit 10 is connected to the electronics apparatus 24 REQUEST line is taken LOW, releasing the reset lines and disabling the pseudo-random sequence generator clock via AND gate 118 and OR gate 120. Counter 114 is clocked via OR gate 122 and once it is reset has been released, it counts until both Q9 and Q10 are HIGH when its clock is disabled via AND gate 124 and OR gate 122. Counter 114 Q9 controls the state of two-to-one line selector 132 and therefore selects either the data in shift register 86 or 88. These comprise first or second four bits of the authorisation code. Initially Counter 114 Q9 is LOW and data from shift register 86 is selected.

As described above the pseudo-random sequence (P.R.S..) generator stops when its clock is inhibited by the LOW reset line. Four bit full adder 130 produces the sum of the four bits of output data (Q0 to Q3) from the PRS and the four bits of data selected from shift register 86. Clearly with more secure systems there would be a greater bit length.

The sum is presented to the first four parallel input lines of shift register 126, the remainder are tied LOW. Data is jammed into register 126 when counter 114 Q8 is HIGH and shifted from QH (synchronous with its clock) when Q8 goes LOW. D type latch 116 and OR gate 128 generate a burst of eight clock pulses following the LOW transition of counter 114 Q8, to clock this data out and provide clock pulses to the electronics apparatus.

The data could of course be transmitted, combined with its clock, as a pulse width modulated data stream just as the battery charger 12 transmits data to the battery unit 10 during charging, via a single connection.

As counter 114 Q8 goes LOW Q9 goes HIGH and clocks the P.R.S. once via OR gate 120, presenting the next four bits of output data to adder 130. Since counter 114 Q9 is now HIGH the data selector 132 is routing the second four bits of authorisation code, from shift register 88, to four bit full adder 130.

The sum of the four bits presented by the P.R.S. and line selector is again presented to shift register 126, jammed in when counter 114 Q8 is HIGH and shifted out from QH as serial data when LOW.

Counter 114 Q9 and Q10 are now high and the clock of counter 114 is disabled via AND gate 124 and OR gate 122 preventing further data transmission until the REQUEST line is allowed to go HIGH and then LOW again (i.e. the battery unit 10 is removed and reconnected to the electronics apparatus 24). Thus the first four bits of code data have been added to a four bit number obtained at random and transmitted with a corresponding number of clock pulses to the electronic apparatus. This has then been followed by the sum of the second four bits of code data and the "random" four bit number which follows in the generated sequence, with their corresponding clock pulses.

Operation of a piece of electronic apparatus will now be described in detail with reference to Figure 4, in which an electronic apparatus 24 comprises electronic means to read a preset authorisation code (numerically the same (in this example) as two four bit codes programmed into the charger 12 and sent to the battery unit 10), and means to add the data to "random numbers" generated by a P.R.S generator and to compare the sum with serial data sent from the battery unit 10 as described above with reference to Figure 3.

An authorisation code is preset by connecting the eight inputs of the two to one line selector 133 either HIGH or LOW. This data would of course be stored in R.O.M. (not shown) in a commercial implementation. When the battery unit 10 is connected, power on reset is generated by inverter 134, resistor 136 and capacitor 138. The first four bits of code data (CODE) are selected and added by a four bit full ADDER 140, to the output of a pseudo-random sequence generator (P.R.S), as described above. The P.R.S is continuously clocked since the NOT Q of "D" type latch 142 is reset HIGH, via AND gate 144.

An oscillator is formed by resistor 146, capacitor 148 and invertor 150. The output of the adder 140 therefore presents a series of 4 bit words representing the sum of the first CODE and the successive outputs of the P.R.S.

Serial data and its clock are presented by battery unit 10 as described above, and loaded into shift register 135. This also clocks monostable 137, which is retriggerable and has a period of twice the incoming clock, so that its NOT Q goes LOW during the receipt of data. At the end of four bits of data, the NOT Q returns HIGH, clocking the Q of D type latch 152 HIGH. The output of AND gate 152 therefore goes HIGH enabling the output of the four bit comparator via AND gate 158. During the receipt of subsequent data the LOW on M/S 1 NOT Q disables comparison via AND gates 154 and 158, to prevent an invalid but correct comparison (occurring due to data corruption during loading) from taking place.

Output of ADDER 140 is compared, using a 4 bit magnitude comparator with the encoded data from the battery unit 10. When the data are the same the output of the comparator 156 goes HIGH and clocks "D" type latch 160 via AND gate 158. Since D1 has not changed state, the Q of "D" type latch 160 remains LOW (i.e. unchanged). The output of the P.R.S. in the electronic apparatus 24 now matches the state of the P.R.S. in the battery unit 10 when it was encoding the first four bits of code. That is the two P.R.S's are synchronised. When the P.R.S has been clocked one step past the output which resulted in equivalence of the sum and input data, the output of the 4 bit comparator 156 goes (back) LOW clocking latch 142 via invertor 162. Latch 142 NOT Q goes LOW and disables the P.R.S. clock. Latch 142 Q goes HIGH and selects the second CODE word via the line selector. The pseudo-random sequence generator therefore stops one step beyond the number which resulted in equivalence, i.e. at the same point as that used by the P.R.S in the battery unit 10 to encode the second CODE. The second electronics apparatus CODE has been selected and the sum therefore anticipates the encoded data expected next from the battery unit 10. When the second piece of encoded data is received from the battery unit it is compared with the output of the ADDER 140 (generated as described above) and if the two codes are the same, or that is the code presented by the battery unit is an authorisation code, comparator 156 output goes HIGH. Latch 160 is therefore clocked, transferring the

HIGH now present on its D input to its Q, indicating that the received data are valid and thereby authorising operation of the electronic apparatus 25.

If a third four bit word is received from the battery unit 10 then D type latch 164 has a HIGH clocked into its Q. Latches 146 and 160 are reset via OR gate 166 preventing authorisation. This may only occur if an unauthorised user were attempting to overcome the system.

Thus two authorisation codes have been sent from the battery charger 12 to the electronic apparatus via the battery unit 10, where both codes have been recognised as valid and thus use of the apparatus is authorised. Both codes are encrypted in such a way as to prevent an unauthorised user who is in possession of BOTH the battery unit and electronics apparatus from successfully interrogating the link between them and identifying the authorisation codes. The electronic apparatus is therefore only of value to a thief until the battery has discharged and is spent. Once this has occurred, unless the thief has knowledge of the codes, recharging the battery will be associated with loss of its stored codes and therefore further use will be prevented. Alternatively the codes stored in the store in the battery unit become erased.

It will be appreciated that the invention has been described by way of an example only and variation to the above embodiment may be made without departing from the scope of the invention.

CLAIMS

1. Apparatus for receiving a removable battery unit, the battery unit comprising a rechargeable battery and a memory store, the apparatus having comparison means for comparing a security code stored in the apparatus, with an authorisation code presented by the memory store and means for selectively enabling the apparatus upon receipt of a valid authorisation code or disabling the apparatus upon receipt of an invalid authorisation code.

2. An electronic apparatus comprising a first data store for storing a code; means for comparing a stored code with a security code received from a second data store and means to enable the electronic apparatus when the security code is a valid authorisation code characterised in that the second data store is supported by or disposed within a detachable rechargeable battery unit.

3. Apparatus according to Claim 1 or 2 wherein the security code stored in the second store is automatically erased when the battery is spent.

4. Apparatus according to Claim 3 in which the code is encrypted.

5. An electronic anti-theft method comprising the steps of: transmitting a security code to a first data store within an electronic apparatus from a second data store, comparing the security code with an already stored code, such that the electronic apparatus is enabled if the security code is a valid authorisation code, characterised in that the second data store, is disposed on or within a detachable rechargeable battery unit.

6. A method according to Claim 5 wherein the security code is transmitted to the apparatus more than once.

7. A method according to either of claims 5 or 6 wherein a security code stored in the second store is automatically erased when the battery is spent.

8. A method according to Claim 7 wherein the battery unit is placed in a battery recharger and a new security code is generated by the battery recharger.

9. A method according to Claim 8 in which the security code is encrypted.

10. A modified battery charger comprising: means for enabling a security code to be entered; means to store said security code; means to supply an electric current in order to recharge a battery unit in electrical contact with the charger and means to transmit said security code to the battery unit whilst the battery is recharging.

11. A battery unit comprising a rechargeable battery and a data store, within which data store a security code is written.

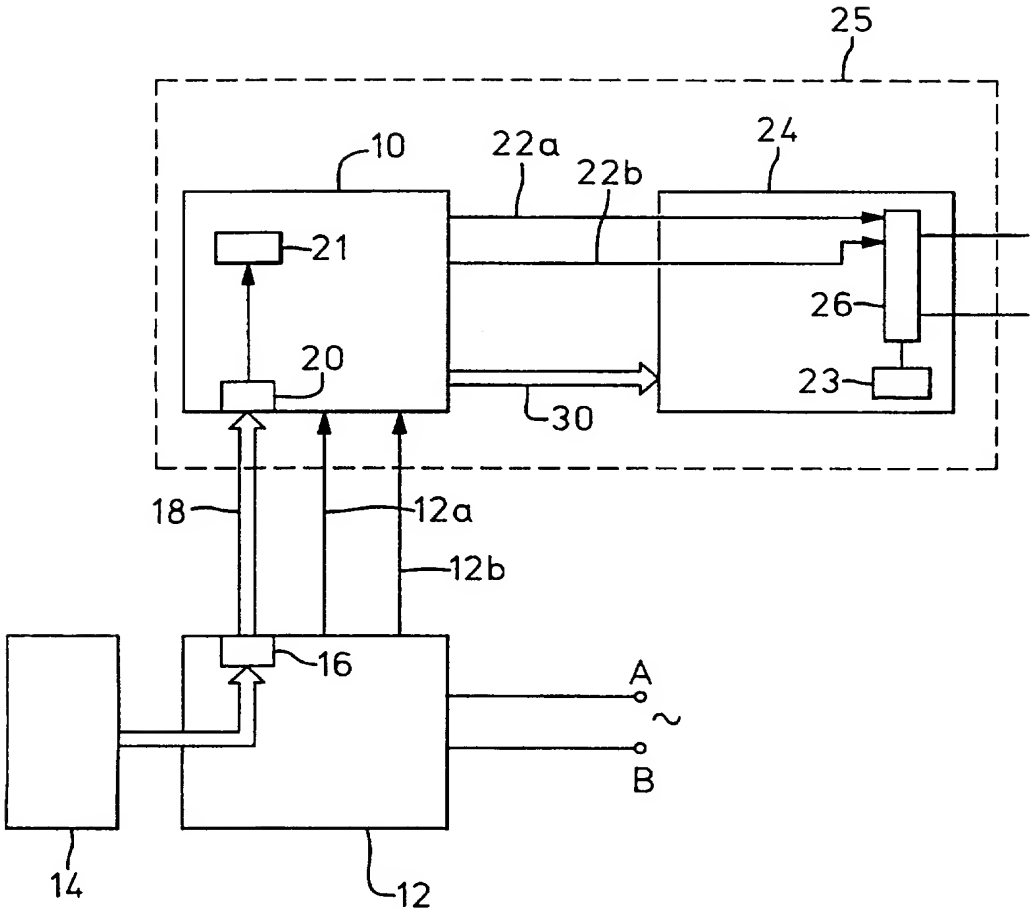


Fig.1

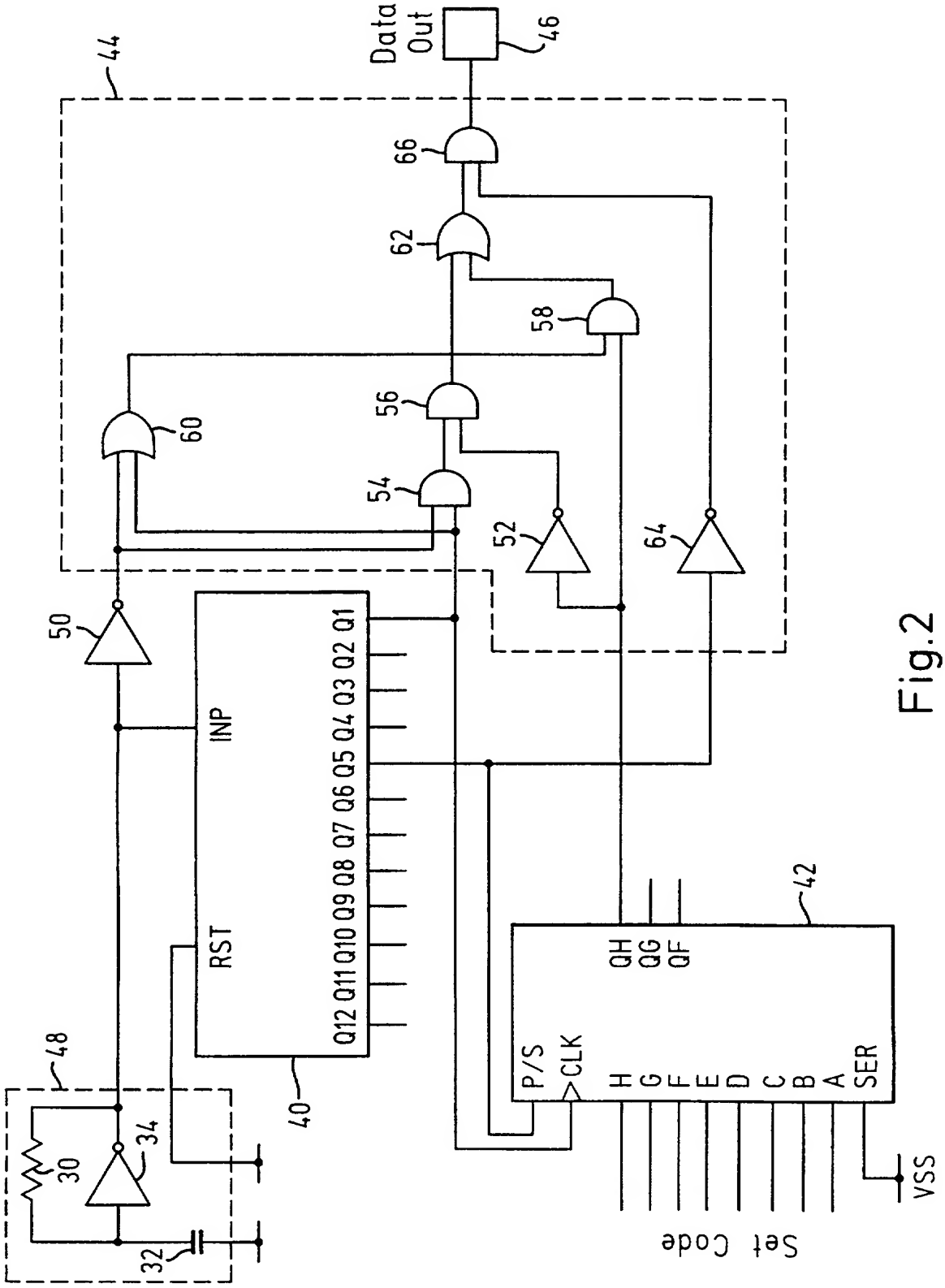

Data Out
46
44
66
62
58
56
60
54
52
64
50
INP
RST
Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10 Q11 Q12
40
42
QH QG QF
P/S
CLK
H G F E D C B A SER
VSS
Set Code
48
30
34
32

Fig.2

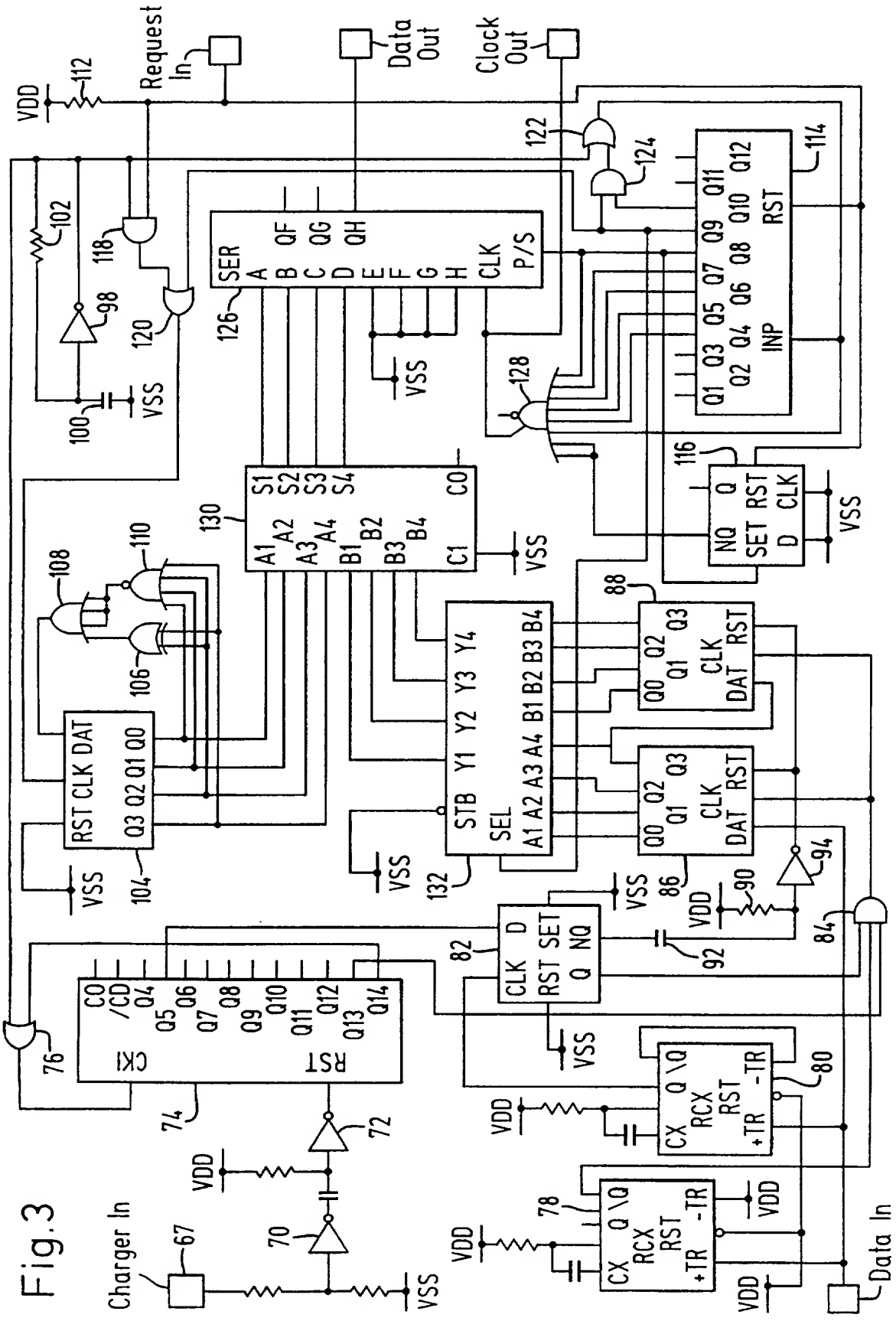

Request In
Data Out
Clock Out
VDD
112
102
118
120
98
100
VSS
122
124
114
126
SER
A
B
C
D
E
F
G
H
QF
QG
QH
CLK
P/S
Q11
Q12
Q9
Q10
Q7
Q8
Q5
Q6
Q3
Q4
Q1
Q2
INP
RST
128
116
NQ
Q
SET
RST
D
CLK
130
S1
S2
S3
S4
A1
A2
A3
A4
B1
B2
B3
B4
C0
C1
108
110
106
104
RST CLK DAT
Q3 Q2 Q1 Q0
88
STB
SEL
Y1
Y2
Y3
Y4
132
86
90
94
84
92
82
CLK
RST
SET
D
Q
NQ
CO
/CO
Q4
Q5
Q6
Q7
Q8
Q9
Q10
Q11
Q12
Q13
Q14
CK
RST
76
74
72
CX
RCX
Q
\Q
+TR
-TR
80
78
Charger In
67
70
Data In

Fig.3

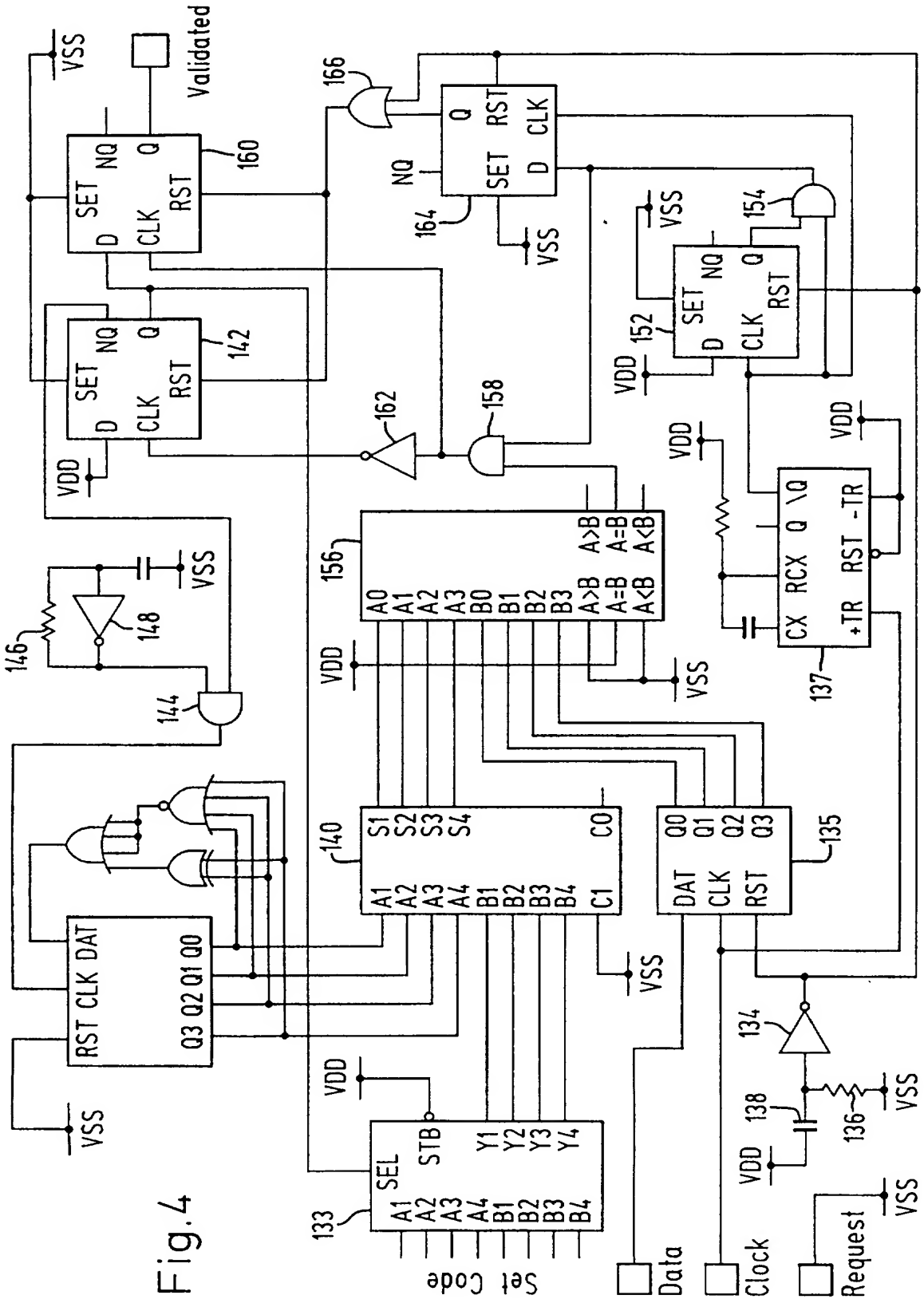

VSS
Validated
160
SET NQ Q
D CLK RST
166
Q RST
NQ SET D CLK
164
VSS
154
VSS
SET NQ Q
152 D CLK RST
VDD
142
SET NQ Q
D CLK RST
VDD
162
158
VDD
VDD
156
A0 A1 A2 A3 B0 B1 B2 B3 A>B A=B A<B
A>B A=B A<B
VDD
VSS
CX RCX Q \Q
+TR RST -TR
137
VSS
148
146
144
140
S1 S2 S3 S4 C0
A1 A2 A3 A4 B1 B2 B3 B4 C1
VSS
Q0 Q1 Q2 Q3
DAT CLK RST
135
RST CLK DAT
Q3 Q2 Q1 Q0
VSS
VDD
134
VSS
138
136
VDD
133
SEL STB Y1 Y2 Y3 Y4
A1 A2 A3 A4 B1 B2 B3 B4
Set Code
Data
Clock
Request
VSS

Fig.4

INTERNATIONAL SEARCH REPORT

Inte nal Application No
PCT/GB 96/03177

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M1/72 G08B13/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04M G08B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 38 03 357 A (PHILIPS PATENTVERWALTUNG) 17 August 1989 see the whole document -----	1-11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
7 March 1997	18. 03. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Sgura, S

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ıal Application No
PCT/GB 96/03177

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 3803357 A	17-08-89	NONE	

PUB-NO: WO009723986A1
DOCUMENT-IDENTIFIER: WO 9723986 A1
TITLE: AN ELECTRONIC ANTI-THEFT APPARATUS AND RELATED METHOD
PUBN-DATE: July 3, 1997

INVENTOR-INFORMATION:

NAME	COUNTRY
SANSOME, ANDREW JONATHAN THOMAS	GB

ASSIGNEE-INFORMATION:

NAME	COUNTRY
BRITISH TECH GROUP	GB
SANSOME ANDREW JONATHAN THOMAS	GB

APPL-NO: GB09603177
APPL-DATE: December 20, 1996

PRIORITY-DATA: GB09526235A (December 21, 1995)

INT-CL (IPC): H04M001/72 , G08B013/14

EUR-CL (EPC): G08B013/14 , H04M001/727

ABSTRACT:

CHG DATE=19990617 STATUS=O>The invention describes an anti-theft apparatus and related method for use with portable electrical or

electronic apparatus, particularly with mobile telephones or personal computers. The invention comprises a first data store in which an encrypted code is stored in the electronic apparatus, a comparator and a removable second data store which is within a removable, rechargeable battery unit which unit comprises a battery and a memory store. Upon insertion of the battery unit a security code is transmitted to the first data store. If the code is recognised as a valid authorisation code, the apparatus is enabled and may be operated in the usual way. If it is not recognised the apparatus may be disabled electronically. Once the battery is spent the apparatus is useless, because unless the battery unit receives a refreshed security code upon recharge (from a recharger equipped with a means for re-supplying a suitable code) the electronic apparatus may not be used. Preferably a recharger has been modified such that a valid security code is transmitted to the battery unit at each recharge.